Data security in multi-carrier communication systems.

Patent Number: ☐ EP0457602, B1

Publication date: 1991-11-21

Inventor(s): HINOKIMOTO SHINICHI (JP)

Applicant(s): FUJITSU LTD (JP)

Requested Patent: ☐ JP4022235

Application Number: EP19910304443 19910517

Priority Number(s): JP19900127606 19900517

IPC Classification: H04J9/00; H04L5/06

EC Classification: H04L9/00, H04N1/44, H04L1/00A1M, H04L27/26M1A1

Equivalents: AU628739, AU7705891, DE69127023D, DE69127023T, JP2761281B2, ☐ US5226081

Cited Documents: WO8607223; US4924516

Abstract

A multi-carrier communication system wherein a sender side apparatus and a receiver side apparatus (10, 11) are connected through a transmission line (12). The sender side apparatus contains a multi-carrier modulator (14, 14 min) for modulating data, where preset numbers of bits of the data are respectively modulated with a plurality of carriers in each cycle. The sender side apparatus transmits a training signal which is modulated by the multi-carrier modulating unit (14, 14 min) where the numbers are set equal to a predetermined maximum of the numbers, to the receiver side apparatus. The receiver side apparatus evaluates the quality of components of the training signal where the components are modulated with the respective carriers to determine the above numbers to be preset, ciphers information on the numbers, and transmits the ciphered information to the sender side apparatus. The sender side apparatus deciphers the information to obtain the determined numbers, and presets the numbers in a multi-carrier demodulator (16, 16 min) which is provided therein.

Reference 3

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4-22235

⑤1Int.Cl.[5]		識別記号	庁内整理番号	⑬公開 平成4年(1992)1月27日
H 04 L	9/00			
	9/10			
	9/12			
H 04 M	11/00	302	7117-5K	
			7117-5K H 04 L 9/00	Z

審査請求 未請求 請求項の数 5 (全13頁)

⑤4発明の名称　マルチキャリア通信システムの暗号化通信方式

⑳特　願 平2-127606
㉒出　願 平2(1990)5月17日

㉑発明者　桧本　晋一　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士 竹内　進　外1名

明細書

1．発明の名称

マルチキャリア通信システムの暗号化通信方式

2．特許請求の範囲

(1) マルチキャリアモデム(10-1, 10-2)を伝送回線(12)を介して接続したマルチキャリア通信システムに於いて、

前記マルチキャリアモデム(10-1, 10-2)の各々に、

伝送帯域内に複数のキャリアを配置し、送信データをキャリア毎に定められたビット数に区切って同時変調して前記伝送回線(12)に送出する変調手段(14)と；

前記伝送回線(12)から受信した変調キャリアから前記各キャリア毎のビットデータを復調して出力する復調手段(16)と；

トレーニング信号を受信した際に前記復調手段(16)の復調出力に基づいて各キャリア毎の伝送ビット数を決定するキャリアビット数判定手段(18)と；

該キャリアビット数判定手段(18)で決定したキャリア毎のビット数情報について予め定められた特定数のキャリアを暗号化して前記変調手段(14)によりトレーニング信号送信側に送信させると共に、前記復調手段(16)で復調された暗号化ビット数情報を解読してキャリア毎のビット数を前記変調部(14)に設定する暗号化手段(20)．；

を備えたことを特徴とするマルチキャリア通信システムの暗号化通信方式。

(2) 請求項1記載のマルチキャリア通信システムの暗号化通信方式に於いて、

前記暗号化手段(20)は、

前記各キャリア毎に割当てられるビット数をnとした時、予め定めた暗号コードのビット数により該ビット数nに(n+1)進数の加算を施して加算結果を相手方に通知させる暗号変換手段と；

受信した(n+1)進数の暗号化ビット数から

前記暗号コードのビット数を減算して各キャリア毎のビット数nを復元する暗号復元手段と；
を備えたことを特徴とする通信システムの暗号化通信方式。

（3）請求項2記載のマルチキャリア通信システムに於いて、
前記暗号化手段(10)は、暗号化されたキャリアビット数情報を（n＋1）進数で表現し、且つ該暗号化を施すキャリアの本数をXとした場合に、
$1/(n+1)^x$
として定義される暗号化率が規定値以下となるように暗号化を施すキャリア本数Xを決定することを特徴とするマルチキャリア通信システムの暗号化方式。

（4）請求項1記載のマルチキャリア通信システムの暗号化通信方式に於いて、
前記変調手段(14)は、キャリア毎のビット数に区切られた送信データをＱＡＭ変調の信号点座標（Ｘｎ，Ｙｎ）に変換した後に、各キャリア周波数に基づく逆フーリエ変換を行って得た１周期分の時系列信号を送信することを特徴とするマルチキャリア通信システムの暗号化通信方式。

（5）請求項1記載のマルチキャリア通信システムの暗号化通信方式に於いて、
前記復調手段(16)は、前記伝送回線(12)から受信した１周期分の受信信号系列をフーリエ変換して各キャリア毎のＱＡＭ変調の信号点座標（Ｘｎ，Ｙｎ）を復元し、該信号点座標（Ｘｎ，Ｙｎ）からビットデータを復元することを特徴とするマルチキャリア通信システムの暗号化通信方式。

3．発明の詳細な説明

［概要］

伝送帯域に多数のキャリアを配置し、キャリア毎のビット割当数に従ったビットデータで同時変調して高速伝送するマルチキャリア通信システムの暗号化通信方式に関し、

簡単に伝送データを暗号化して守秘性を確保することを目的とし、
トレーニング受信により各キャリア毎の割当ビット数を決定して相手方に送信する際に、割当ビット情報に暗号コードを加算する暗号化を施すことで、第3者による受信を不能にするように構成する。

［産業上の利用分野］

本発明は、伝送帯域に多数のキャリアを配置し、キャリア毎のビット割当数に従ったビットデータで同時変調して高速伝送するマルチキャリア通信システムの暗号化通信方式に関する。

近年、データ伝送は日常茶飯事に行われているが、近年になってデータ（情報）の盗聴問題がクローズアップされている。

例えばファクシミリ装置の普及により重要な書類をファクシミリ伝送する機会も増えているが、産業スパイ等がこれを盗聴し、さらにファクシミリ装置により電文を出力させることが比較的容易にできることが知れらている。

このような場合に、何らかの秘話対策が必要となる。

［従来技術］

従来、電話回線を使用したデータ伝送システムにあっては、モデムに１本のキャリア（半二重通信）又は２本のキャリア（全二重通信）を割当て、このキャリアを送信データに基づく例えばＱＡＭ方式により変調して送信し、受信側で復調している。データ伝送速度は変調速度を一定とすると１変調当りのビット数で決まり、ビット数を増加させるためにはＱＡＭ変調の信号点の数を増加しなければならない。しかし、実用可能な信号点数には限界があり、高速伝送のネックとなっている。

このような従来のモデムを使用したデータ伝送における秘話対策としては、高価な暗号機を購入するか、あるいは重要な書類は郵送や人の手によって運ぶといった方法が取られている。

[発明が解決しようとする課題]

しかしながら、暗号機の使用は極めて専門的且つ特殊な用途であり、重要な情報だからといってファクシミリ伝送等の日常的なデータ通信に使用することは事実上不可能である。

一方、近年においてマルチキャリア通信システムとして知られた高速通信方式が知られている。

このマルチキャリア通信システムに使用するモデムは、伝送帯域に多数のキャリアを配置し、キャリア毎に回線品質に応じたビット数を割当て、各キャリアをビットデータで同時にＱＡＭ変調して伝送回線に送出する。

例えば０～４０００Ｈｚの伝送帯域に５１２本のキャリアを配置し、実用伝送帯域３００～３４００Ｈｚでは４００本程度のキャリアを確保でき、理想的な状態では１８Ｋビット／秒の高速通信速度が得られる。

このマルチキャリアモデムでは、受信側でキャリア毎の回線品質を監視して伝送可能なキャリアビット数を決め、このキャリアビット数を送信側に送ってキャリア毎のビット割当数を設定するようにしている。

従って、受信側で決定したビット数割当て情報が分からなければ正常なデータ通信はできない。

本発明は、このようなマルチキャリア通信システムに着目して成されたもので、マルチキャリア通信システムの技術を利用して解読困難な暗号化を安価に実現できるマルチキャリア通信システムの暗号化通信方式を提供することを目的とする。

[課題を解決するための手段]

第１図は本発明の原理説明図である。

まず本発明は、マルチキャリアモデム１０－１，１０－２を伝送回線１２を介して接続したマルチキャリア通信システムを対象とする。

このようなマルチキャリア通信システムのマルチキャリアモデム１０－１，１０－２は、伝送帯域内に複数のキャリア周波数を配置し、送信データをキャリア毎に定められたビット数に区切って同時変調して前記伝送回線１２に送出する変調手段１４と、伝送回線１２から受信した変調キャリアから各キャリア毎のビットデータを復調して出力する復調手段１６と、トレーニング信号を受信した際に復調手段１６の復調信号に基づいて各キャリア毎のキャリアビット数を決定して相手方に通知するキャリアビット数判定手段１８とを備える。

このようなマルチキャリア通信システムに対し本発明にあっては、マルチキャリアモデム１０－１，１０－２のキャリアビット数判定手段１８で決定したキャリア毎のビット数情報について予め定められた特定数のキャリアを暗号化して変調手段１４によりトレーニング信号送信側に通知させると共に、復調手段１６で復調された暗号化ビット数情報を解読してキャリア毎のビット数を変調手段１４に設定する暗号化手段２０を新たに設けたものである。

マルチキャリアモデム１０－１，１０－２に設けられる暗号化手段２０は、各キャリア毎に割当てられるビット数をｎとした時、予め定めた暗号コードにより該ビット数ｎに（ｎ＋１）進数の加算を施して加算結果を相手型に通知させる暗号変換手段と、受信した（ｎ＋１）進数の暗号化ビット数から前記暗号コードのビット数を減算して各キャリア毎のビット数ｎを復元する暗号復元手段とを備える。

例えば暗号化手段２０は、各キャリア毎に割当てられる最大ビット数を７ビットとした時、同じく最大ビット数が７ビットとなる予め定めた暗号コードのビット数に加算を施して８進数の加算結果を相手方に通知させる暗号変換手段と、受信した８進数の暗号化ビット数から前記暗号コードのビット数を減算して最大７ビットとなる各キャリア毎のビット数を復元する暗号復元手段とを備える。

更に暗号化手段２０は、予め定めた特定数のキャリアに対しビット数の暗号化と暗号解読を行なえばよい。具体的には暗号コードを０とすることで暗号化と解読を不要にできる。

更にまた、暗号化手段(20)は、暗号化されたキ

ャリアビット数情報を（n＋1）進数で表現し、且つ該暗号化を施すキャリアの本数をXとした場合に、

$1/(n+1)^X$

として定義される暗号化率が規定値以下となるように暗号化を施すキャリア本数Xを決定する。

一方、マルチキャリアモデム10－1，10－2の変調手段14は，キャリア毎の割当ビット数に区切られた送信データをQAM変調の信号点座標（Xn，Yn）に変換した後に、各キャリア周波数に基づく逆フーリエ変換を行って得た1周期分の時系列信号を送信する。

更にマルチキャリアモデム10－1，10－2の復調手段16は、伝送回線12から受信したの1周期分の受信信号系列をフーリエ変換して各キャリア毎のQAM変調の信号点座標（Xn，Yn）を復元し、該信号点座標（Xn，Yn）からビットデータを復元する。

〔作用〕

このような構成を備えた本発明によるマルチキャリア通信システムの暗号化通信方式によれば、第1図（b）のように、暗号化された伝送コードを（n＋1）進数で表現しているため、暗号化を行うキャリアの本数をX本とした場合、無作為に試行した時の暗号が解ける確率として定義される暗号化率は、

$1/(n+1)^X$

となる。

例えばキャリアビット数nをn＝7ビット、キャリア本数XをX＝12本とした場合、暗号化率は、約0.15×10^{-12}となる。この数値は、事実上、解読負荷可能な十分に暗号化を達成しており、略完全な守秘対策を実現できる。

〔実施例〕

第2図は本発明の一実施例を示した実施例構成図である。

第2図において、10－1，10－2はマルチキャリアモデムであり、アナログ公衆電話回線12を介して接続される。公衆電話回線12は300～3400Hzの伝送帯域をもつ。

マルチキャリアモデム10－1，10－2には変調部14と復調部16が設けられ、変調部14の出力と復調部16の入力はハイブリッドトランス等を用いた切替器22を介して公衆電話回線12に接続される。

変調部14は第3図に示すように公衆電話回線12の伝送回線300Hz～3．4KHz内に複数のキャリア（搬送波）を配置し、送信データSDをキャリアビットアサイメントによりキャリア毎に定められたビット割当て数に区切ってQAM方式（直交振幅変調方式）により同時変調して伝送回線12に送出する。この変調部12によるマルチキャリア変調は、後の説明で明らかにするように、フーリエ逆変換により実現される。

復調部16は切替器22を介して公衆電話回線12から受信した変調キャリアから各キャリア毎のビットデータを復調して受信データRDとして出力する。この復調部16にも第3図（b）に示すように、同図（a）に示す送信側と同じキャリアビットアサイメントによるキャリア毎のビット割当て数が設定されおり、このビット割当て数に基づいて受信した変調キャリアを復調することができる。

更に、マルチキャリアモデム10－1，10－2にはキャリアビットアサイメント判定部18が設けられる。キャリアビットアサイメント判定部18は通信開始時に受信側に位置するキャリアビットアサイメント判定部18が機能し、送信側から最初に送られてくるトレーニング信号を受信した際の復調部16からの復調出力に基づき、各キャリア毎の伝送ビット数を決定するキャリアビット数判定手段としての機能を有する。

例えば第2図において、マルチキャリアモデム10－1を送信側、マルチキャリアモデム10－2を受信側とすると、通信開始時にマルチキャリアモデム10－1からまずトレーニング信号が送出されて受信側のマルチキャリアモデム10－2で受信され、このトレーニング信号の復調部16

からの復調出力に基づき、キャリアビットアサイメント判定部１８で伝送品質に基づいてキャリア毎のビット割当て数を判定し、変調部１４によりキャリアビットアサイメント情報を変調して送信側のマルチキャリアモデム１０－１に通知してくる。

本発明にあっては、この受信側から送信側に対するキャリアビットアサイメント情報の通知について暗号化を施すことを特徴とする。

即ち、マルチキャリアモデム１０－１，１０－２のキャリアビットアサイメント判定部１８の出力は暗号化部２０に与えられ、暗号化部２０において外部設定された暗号コードＣＤにより暗号化され、暗号化されたキャリアビットアサイメント情報を変調部１４よりトレーニング信号送信側に通知するようになる。

同時に、暗号化部２０は相手側から暗号化されて送られてきたキャリアビットアサイメント情報を解読する暗号解読機能を有する。

暗号化部２０による暗号化及び暗号解読を、第４図を参照して説明すると次のようになる。

第４図（ａ）キャリアビットアサイメント情報の送信側、即ちトレーニング信号の受信側で行なわれる暗号化処理を示す。

今、図示のように伝送帯域３００Ｈｚ～３．４ＫＨｚに所定周波数間隔で１～ｎ本のキャリアが配置されており、トレーニング信号の受信に基づきキャリアビットアサイメント判定部１８で各キャリア毎のビットアサイメントＢＮ１～ＢＮｎとして図示のように「５，６，７，・・・，７，７，３」が決定されたとする。

このキャリアビットアサイメントＢＮ１～ＢＮｎに対し同じ最大ビット数７をもつ数値０～７を使用した暗号コードＣＤ１～ＣＤｎが予め設定されている。

暗号化部２０はキャリアビットアサイメントＢＮ１～ＢＮｎに暗号コードＣＤ１～ＣＤｎを加算する暗号化処理を施し、最大ビット数７に１を加えた８進数の暗号化されたキャリアビットアサイメント、即ち伝送コードＣＢＮ１～ＣＢＮｎを生成し、これを相手先に送信する。具体的には、暗号コードＣＤ１～ＣＤｎとして「４，５，２，・・・，０，７，１」が設定されていたとすると、キャリアビットアサイメントＢＮ１～ＢＮｎの各キャリア毎のビット数値とコード数値の加算によりＣＢＮ１～ＣＢＮｎとして「１，３，１，・・・，７，６，４」を得ることができる。

一方、第４図（ｂ）の受信側にあっては、送信側と同じ暗号コードＣＤ１～ＣＤｎとして「４，５，２，・・・，０，７，１」が設定されており、受信した伝送コードＣＢＮ１～ＣＢＮｎ「１，３，１，・・・，７，６，４」に対し暗号コードＣＤ１～ＣＤｎによる逆算、即ち減算を施すことにより解読し、正しいキャリアビットアサイメントＢＮ１～ＢＮｎとして「５，６，７，・・・，７，７，３」を再現することができる。

この第４図に示す暗号化及び暗号解読を更に一般的に述べるならば、各キャリア毎に割り当てられるキャリアビットアサイメントのビット数をｎとしたとき、予め定めた暗号コードのビット数によりキャリアビットアサイメントのビット数ｎに（ｎ＋１）進数の加算を施して加算結果を相手方に通知させる暗号変換を行なう。一方、暗号復元（暗号解読）については、受信した（ｎ＋１）進数の暗号化ビット数から送信側と同じ暗号コードのビット数を減算して各キャリア毎のビット数ｎを復元することになる。

このように、キャリアビットアサイメントのビット数ｎに暗号コードによる加算を施して（ｎ＋１）進数で表現する暗号化にあっては、暗号化を行なうキャリアの本数をＸとした場合、暗号化率（無作為に試行したときの暗号が解ける確率）は、

$$1/(n+1)^X$$

となる。

例えば、キャリアビットアサイメントのビット数ｎをｎ＝７ビット、暗号化を行なうキャリアの本数ＸをＸ＝１２本としたときの暗号化率は約0.15×10^{-12}となる。この暗号化率の数値は実用上解読不可能といえる十分な暗号化を達成した数値といえる。

ここで、第4図に示す暗号コードの中の数値0については、キャリアビットアサイメントに暗号コードを加算しても、結果として得られる暗号コードは同じ値であり、従って暗号コード0については暗号化が行なわれていないことを意味する。

従って、例えば前述したようにキャリアビット数n＝7ビット、暗号化を行なうキャリア本数X＝12とした場合には、キャリアビットアサイメントの中の割当てビット数が7となる12本のキャリアを選択し、選択した12本のキャリアに対応する暗号コードの値として1～7の数値を割り当て、選択した12本以外のキャリアについては暗号コード0を設定するようにしてもよい。このような特定のキャリアについてのみ有効暗号数値1～7を加えられることで、暗号化のための加算、及び暗号解読のための減算処理量を低減して高速処理を図ることができる。即ち、暗号化及び暗号解読において暗号コードが無効数値0となる部分については加算または減算を行なわさせずにキャリアビットアサイメントをそのまま暗号コードまたは解読コードとして使用できるからである。

勿論、キャリアビットアサイメントの全てについて有効暗号数値1～7を割り当てるようにしてもよいことは勿論である。

次に、第2図の実施例における通信処理を第5図のタイミングチャートを参照して説明する。

今、マルチキャリアモデム10－1からマルチキャリアモデム10－2に、ある送信データSDを送信するものとする。送信側のマルチキャリアモデム10－1からの呼出しにより受信側のマルチキャリアモデム10－2の公衆電話回線12に対する接続が確立すると、送信側のマルチキャリアモデム10－1はまずトレーニング信号を送信する。このトレーニング信号は複数のキャリアを配置した300Hz～3．4KHzの全域に亘ってフラットな信号となる。尚、トレーニング信号送出時の各キャリア毎のキャリアビットアサイメントの値は、例えば全てのキャリアについて最大ビット数7が割り当てられている。

モデム10－1からのトレーニング信号TRNは受信側のマルチキャリアモデム10－2の復調部16で復調され、各キャリア毎の復調出力、具体的にはQAM方式の信号点座標を示すベクトル成分（Xi，Yi）がキャリアビットアサイメント判定部18に与えられる。但し、i＝1～nでキャリア番号を示す。キャリアビットアサイメント判定部18はキャリア毎のトレーニング信号復調出力から伝送劣化の度合いを判断し、伝送品質に応じたビット割当て数、即ちキャリアビットアサイメントBN1～BNnを設定する。尚、割当てビット数が0となるキャリアは使用されないことを意味する。

キャリアビットアサイメント判定部18で決定されたキャリアビットアサイメント情報BN1～BNnは暗号化部20に与えられ、第4図（a）に示したように予め設定された暗号コードCD1～CDnによる加算が施され、（n＋1）進数としての加算結果が暗号化コードCBN1～CBNnとして変調部14に与えられ、変調部14で変調してキャリアビットアサイメントCAとしてトレーニング信号を送信したマルチキャリアモデム10－1に通知する。受信側からのキャリアビットアサイメントCAはマルチキャリアモデム10－1の復調部16で受信データRDとして復調され、暗号化部20に与えられる。暗号化部20は受信したキャリアビットアサイメント情報CBN1～CBNnに対し、第4図（b）に示すように、文字暗号コードCD1～CDnを使用した減算を施すことで、正しいキャリアビットアサイメントBN1～BNnを解読し、この解読結果を変調部14及び復調部16に設定する。

尚、受信側のマルチキャリアモデム10－2のキャリアビットアサイメント判定部18は、決定したキャリアビットアサイメント情報BN1～BNnを暗号化して、トレーニング信号送信先に通知した後、自らの変調部14及び復調部16に対しても決定したキャリアビットアサイメント情報BN1～BNnを設定する。

このようなトレーニング信号TRNに対するキャリアビットアサイメントCAの応答によりモデ

ム）10－1，10－2の変調部14及び復調部16にはそのときの公衆電話回線12の伝送品質に基づくキャリア毎の割当てビット数BN1～BNnが共通に設定された通信可能状態となる。続いて、送信側のマルチキャリアモデム10－1の変調部14は同期信号SYNを送信して受信側のマルチキャリアモデム10－2との同期を確立し、同期信号SYNに続いて送信データSDでマルチキャリア変調を行なって、マルチキャリアモデム10－2側に送信するようになる。

第6図は第2図のモデム10－1，10－2に設けられた変調部14の実施例構成図である。

第6図において、変調部14の入力側には切替スイッチ24が設けられ、切替スイッチ24の切替端子Aには外部から送信データSDが与えられ、切替端子Bには同期信号発生器26から同期信号SYNが与えられ、切替端子Cには暗号化部20より暗号化されたキャリアビットアサイメント情報CBN1～CBNnが与えられている。切替スイッチ24はトレーニング信号受信時に切替端子Cに切り替わって暗号化部20からの暗号化されたキャリアビットアサイメント情報CBN1～CBNnを入力する。また、送信開始時に切替端子Bに切り替わって同期信号発生器26からの同期信号SYNを入力する。同期信号SYNの送信が終了すると切替端子Aに切り替わって送信データSDを取り込む。

切替スイッチ24に続いてはバッファメモリ（以下単に「バッファ」という）28が設けられ、1回の送信分の送信データSDの送信ビットb1～bnが格納される。バッファ28に続いては信号点ベクトル発生部30が設けられる。信号点ベクトル発生部30に対してはキャリアビットアサイメント判定部18（受信側モデムの場合）、または暗号化部20（送信側モデムの場合）からキャリアビットアサイメント情報BN1～BNnが与えられている。信号点ベクトル発生部30はキャリアビットアサイメント情報BN1～BNnに基づく各キャリア毎の割当てビット数に従ってQAM方式における信号点数を判別し、信号点数に対応して予め準備されているマッピング回路を選択し、割当てビット数分の送信データビットをバッファ28から引き出してマッピング回路により信号点座標（Xi，Yi）で成るベクトル成分を発生する。

例えば、割当てビット数0については使用しないキャリアと判別し、ビット数2では信号点数4のマッピング回路を選択し、割当てビット数3では信号点数16のマッピング回路を選択し、割当てビット数4では信号点数32のマッピング回路を選択し、ビット数5では信号点数64のマッピング回路を選択し、ビット数6では信号点数128のマッピング回路を選択し、更に割当てビット数7では信号点数256のマッピング回路を選択する。

信号点ベクトル発生部30で各キャリア毎に発生された信号点ベクトル成分（X1，Y1）～（Xn，Yn）はベクトルテーブルバッファ32に格納される。ベクトルテーブルバッファ32に続いては切替スイッチ34が設けられ、切替スイッチ34はトレーニング信号発生器36の出力とベクトルテーブルバッファ32の出力を替える。即ち、送信側モデムの最初の送信開始時に切替スイッチ34を切替端子Aに切り替えてトレーニング信号発生器36からのトレーニング信号TRNを選択する。トレーニング信号発生器36からのトレーニング信号TRNは信号点座標の特定の信号点（Xo，Yo）に固定したベクトル成分であり、全てのキャリアについて同じ信号点ベクトルによる変調を行なうことになる。

トレーニング信号の送出により相手先からキャリアビットアサイメントが受信されて信号点ベクトル発生部30に対し正しいキャリアビットアサイメント情報BN1～BNnが設定された後の送信時には、切替スイッチ34は切替端子B側に切り替えられ、ベクトルテーブルバッファ32に格納された各キャリア毎の信号点ベクトル成分（X1，Y1）～（Xn，Yn）を順次取り出す。

切替スイッチ34の出力は逆フーリエ変換部38に与えられる。

逆フーリエ変換部３８は伝送帯域に設定されたキャリア周波数と各キャリア毎のベクトル成分、即ち実数成分Ｘｉと虚数成分Ｙｉとに基づく逆フーリエ変換を行なって１周期分の時系列信号を発生する。

具体的に説明すると、逆フーリエ変換のために０～４ＫＨｚの伝送帯域に例えば1.8125Ｈｚ間隔で５１２本のキャリアを配置し、基本周波数を1.8125Ｈｚとして残り５１１本のキャリアを２次～５１２次の高次周波数とし、１次から５１２次の実数成分Ｘ１～Ｘｎと虚数成分Ｙ１～Ｙｎとに基づく逆フーリエ変換により例えば１０２４のフーリエ変換ポイントを示す時系列データを作り出す。

逆フーリエ変換部３８で生成された時系列データＤ１～Ｄ２ｎは時系列バッファ４０に格納される。そして、最終的にＤ／Ａコンバータ４２により１周期分のアナログＱＡＭ信号波形に変換して公衆電話回線に送出するようになる。

第７図は第２図のマルチキャリアモデム１０－１，１０－２に設けられた復調部１６の実施例構成図である。

第７図において、復調部１６はＤ／Ａコンバータ４４、受信時系列バッファ４６、フーリエ変換部４８、受信ベクトルテーブルバッファ５０、ビット列発生部５２及び受信バッファ５４で構成される。

即ち、公衆電話回線５２から受信されたアナログ波形はＤ／Ａコンバータ４４に与えられ、Ｄ／Ａコンバータ４４は入力したアナログ波形をフーリエ変換のピッチ周期を１０２４点に分けてサンプリングしてデジタルデータに変換し、１０２４点の時系列データＤ１～Ｄ２ｎとして受信時系列バッファ４６に格納する。受信時系列バッファ４６に格納された１０２４点のサンプリングデータはフーリエ変換部４８によるフーリエ変換で各キャリア周波数毎のベクトル成分（Ｘ１，Ｙ１）～（Ｘｎ，Ｙｎ）に変換されて受信ベクトルテーブルバッファ５０に格納される。

受信ベクトルテーブルバッファ５０の格納データは順次ビット列発生部５２に与えられ、ビット列の復調が行なわれる。即ち、ビット列発生部５２に対しては各キャリア毎のビット数を示すキャリアビットアサイメント情報ＢＮ１～ＢＮｎがキャリアビットアサイメント判定部１８（受信側の場合）または暗号化部２０（送信側の場合）から設定されており、例えば最初の信号点ベクトル成分（Ｘ１，Ｙ１）のビット割当て数がＢＮ１＝４ビットであったとすると、信号点数１６の逆ビットマッピング変換回路を選択し、４ビットデータを復元して受信バッファ５４に格納する。受信バッファ５４に１回のマルチキャリア通信で得られたベクトル分のビットデータが格納されるか、ある所定量のビットデータが格納されると、順次受信データＲＤとして出力される。

第８図は第２図のマルチキャリアモデム１０－１，１０－２に設けられキャリアビットアサイメント判定部１８の実施例構成図である。

第８図において、キャリアビットアサイメント判定部１８は基準ベクトル発生器５６、割算器５８，６０、ビット数判定部６２及びビットアサイメントバッファ６４で構成される。

基準ベクトル発生器５６はトレーニング信号の信号点座標（Ｘｏ，Ｙｏ）を発生して割算器５８，６０に出力する。割算器５８は実数ベクトル成分Ｘｉ用に設けられ、また割算器６０はベクトル虚数成分Ｙｉ用に設けられている。割算器５８，６０に対しては第７図の復調部１６に設けられた受信ベクトルテーブルバッファ５０に格納されたトレーニング信号受信時の信号点ベクトル成分（Ｘ１，Ｙ１）～（Ｘｎ，Ｙｎ）が順次与えられる。

このようなトレーニング信号の受信に基づく信号点ベクトル成分（Ｘｉ，Ｙｉ）を基準ベクトル発生部５６からの基準ベクトル成分（Ｘｏ，Ｙｏ）のそれぞれで割ることにより、割算器５８，６０から正規化されたベクトル成分をビット数判定部６２に出力する。

ビット数判定部６２は、例えば第９図に示すような判定処理に基づいて各キャリア毎の割当てビット数ＢＮｉを決定する。

第９図において、ベクトル６６は基準ベクトル

成分（Ｘｏ，Ｙｏ）で定まる正規化された基準ベクトルであり、基準ベクトル６６の先端で決まる信号点６８を中心に各ビット毎に許容エラー領域を設定している。即ち、信号点数が２５６となる７ビット領域が最も狭く、６ビット領域、５ビット領域、４ビット領域と順次領域が広がっている。

今、任意のキャリアに対応したトレーニング信号の受信ベクトル成分（Ｘｉ，Ｙｉ）の基準ベクトルに基づく正規化ベクトルが破線のベクトル７０であり、図示のように信号点７２が６ビット領域と５ビット領域の間に位置した場合、このベクトル７０が得られたキャリアについてはビット数５を割り当てる。具体的には、基準ベクトル６６に対する受信ベクトル７０の距離差で与えられる硬判定エラーを求め、この硬判定エラーが１～７ビットの許容エラー範囲に収まるか否かでキャリア毎のビット割当て数を決定する。

尚、第９図の場合には信号点座標の特定信号点（Ｘｏ，Ｙｏ）についてのみトレーニング信号を送ってキャリアビットアサイメントを決定しているが、信号点座標の各象現について定められた信号点Ａ，Ｂ，Ｃ，Ｄを順次トレーニング信号として送り、各象現で決定された割当てビット数を総合的に判断してキャリア毎の割当てビット数を決めるようにしてもよい。

第１０図は第２図のマルチキャリアモデム１０－１，１０－２に設けられた暗号化部２０の実施例構成図である。

第１０図において、暗号化部２０には加算器７４と減算器７６が設けられる。加算器７４及び減算器７６に対しては、予め設定したキャリア本数分の暗号データＣＤ１～ＣＤｎが与えられている。加算器７４は暗号変換手段としての機能をもち、トレーニング信号の受信側のキャリアビットアサイメント判定部１８で得られた送信キャリアビットアサイメント信号ＢＮ１～ＢＮｎを入力して、第４図（ａ）に示した加算処理結果を変調部１４に出力してトレーニング信号送信側に通知する。

一方、減算器７６は暗号解読手段としての機能を有し、トレーニング信号の送出に対し相手方から通知されてきた受信キャリアビットアサイメント信号ＣＢＮ１～ＣＢＮｎを入力して第４図（ｂ）に示すように暗号データＣＤ１～ＣＤｎによる減算を施して正しいキャリアビットアサイメント情報を復元して復調部１６及び変調部１４に設定する。このように、本発明におけるキャリアビットアサイメントの暗号化及び暗号解読は暗号データの加算または減算であることから、ハード構成及び処理が極めて簡単にできる。

［発明の効果］

以上説明してきたように、本発明によれば、トレーニング信号に基づいて決定されるキャリアビットアサイメント情報を暗号化して相手先に送って暗号解読により送信側及び受信側で回線品質に応じた各キャリア毎のビット数割当てを行なっているため、暗号コードが分からない第３者がキャリアビットアサイメントを受信してビット割当て数を設定しても、割当てビット数自体が暗号化されているため、その後に送信されるデータを受信復調しても有効な受信データは得られず、データ伝送の発展に伴い増大する秘話性の要求に大きく寄与することができる。

また、キャリアビットアサイメントの暗号化は暗号コードの加算、解読は暗号コードの減算という簡単な処理で済み、暗号化を行なうキャリアの本数を増やすことにより解読不能な暗号化を簡単に実現することができる。

４．図面の簡単な説明

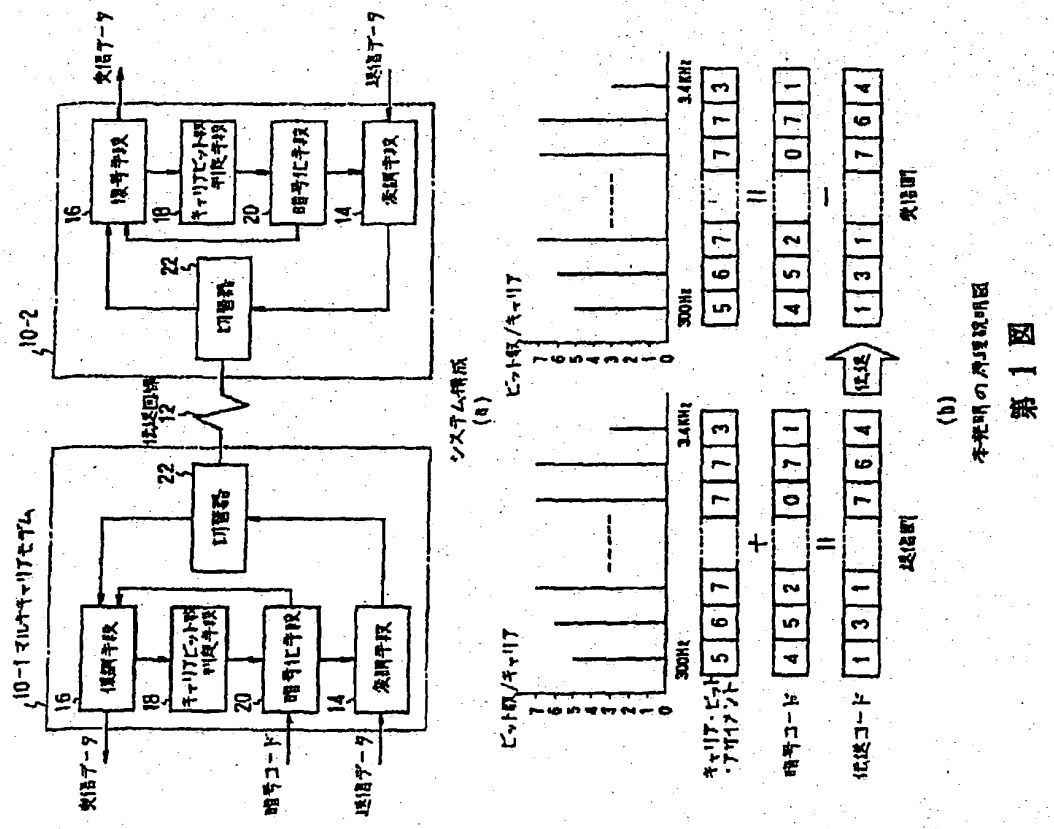
第１図は本発明の原理説明図；
第２図は本発明の実施例構成図；
第３図は本発明のマルチキャリア通信の説明図；
第４図は本発明の暗号化及び暗号解読説明図；
第５図は本発明の通信タイミングチャート；
第６図は本発明の変調部実施例構成図；
第７図は本発明の復調部実施例構成図；
第８図は本発明のキャリアビットアサイメント判定部の実施例構成図；
第９図は第８図のビット数判定処理の説明図；

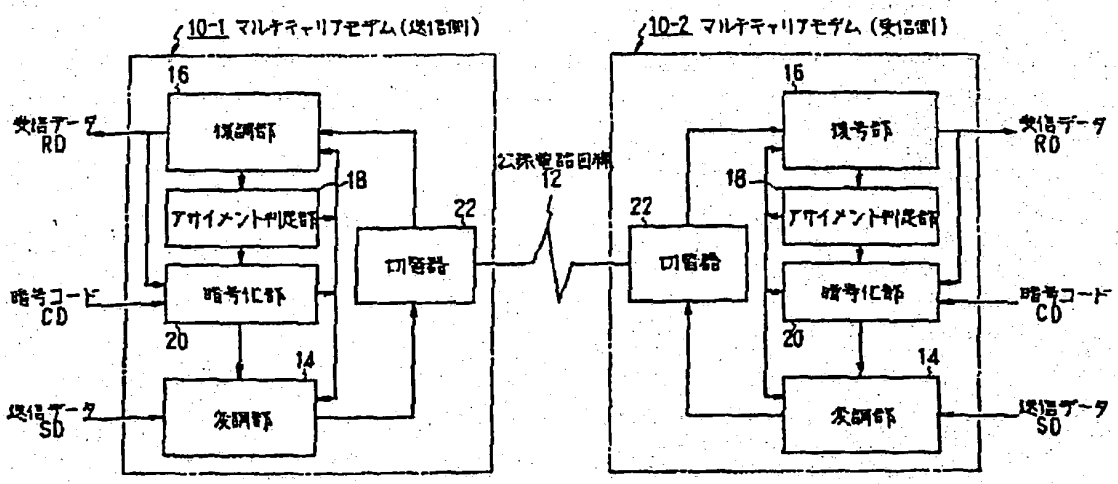
第１０図は本発明の暗号化部実施例構成図である。

図中、

１０－１，１０－２：マルチキャリアモデム
１２：伝送回線（公衆電話回線）
１４：変調手段（変調部）
１６：復調手段（復調部）
１８：キャリアビット数判定手段
（キャリアビットアサイメント判定部）
２０：暗号化手段（暗号化部）
２２：切替器
２４，３４：切替スイッチ
２６：同期信号発生器
２８：バッファ
３０：信号点ベクトル発生部
３２：ベクトルバッファ
３６：トレーニング信号発生器
３８：逆フーリエ変換部
４０：時系列バッファ
４２：Ｄ／Ａコンバータ
４４：Ａ／Ｄコンバータ
４６：受信時系列バッファ
４８：フーリエ変換部
５０：受信ベクトルバッファ
５２：ビット列発生部
５４：受信バッファ
５６：基準ベクトル発生器
５８，６０：演算器
６２：ビット数判定部
６４：ビットキャリアアサイメント・バッファ
６６：基準ベクトル
７０：受信ベクトル
７４：加算器
７６：減算器

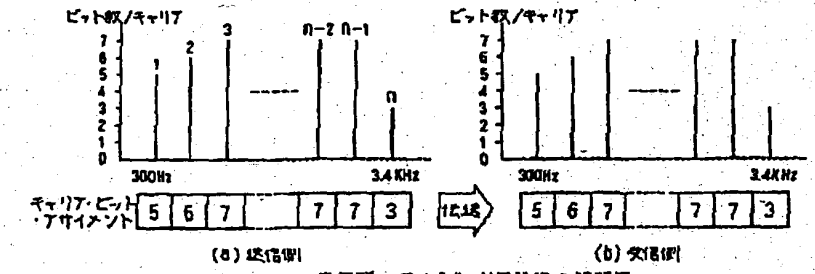
特許出願人　富士通株式会社
代理人　弁理士　竹　内　　進
代理人　弁理士　宮　内　佐一郎





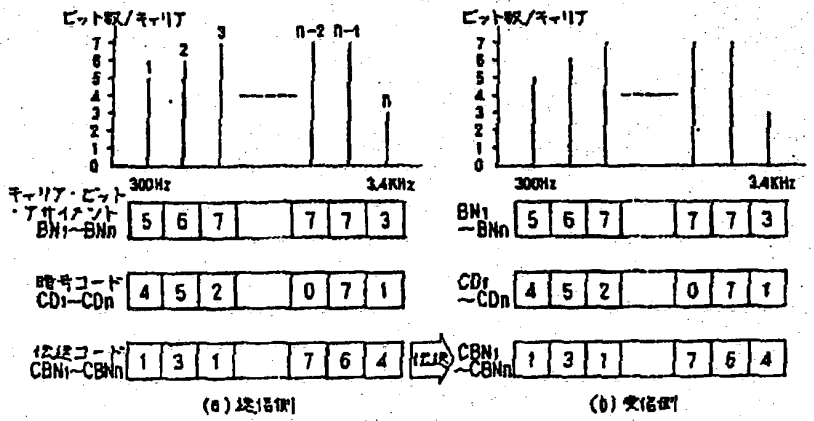
本発明の実施例構成図

第 2 図



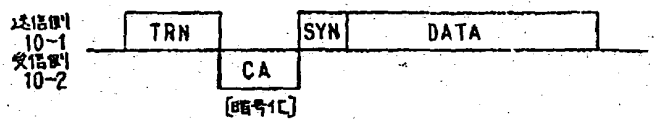
本発明のマルチキャリア通信の説明図

第 3 図



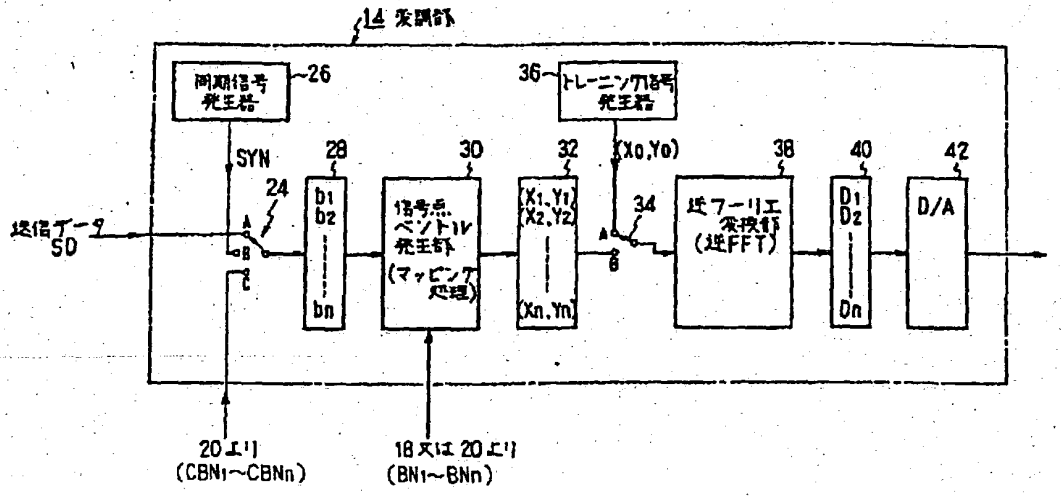
本発明の暗号化及び暗号解読説明図

第 4 図



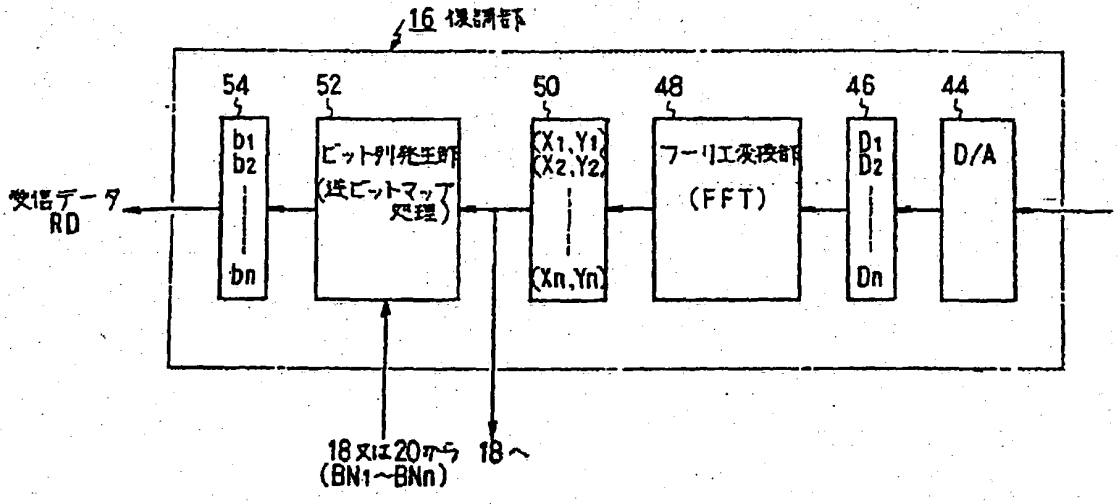
本発明の通信タイミングチャート

第 5 図



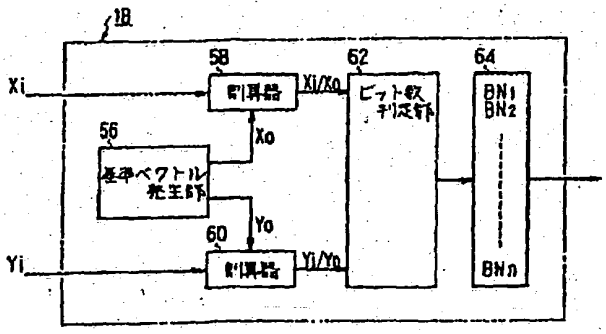
本発明の変調部実施例構成図

第 6 図



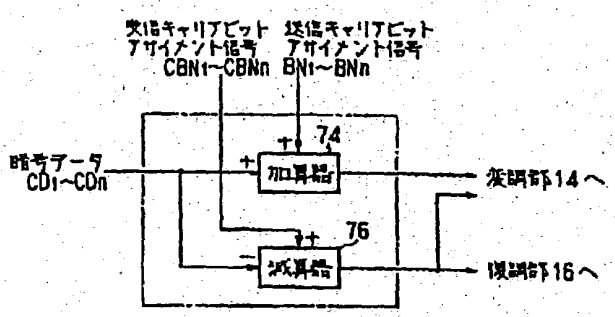
本発明の復調部実施例構成図

第 7 図



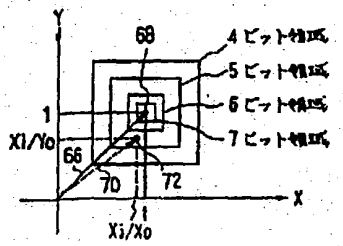
本発明のキャリアビットアサイメント判定部の実施例構成図

第 8 図



本発明の暗号化部実施例構成図

第 10 図



第8図のビット数判定処理の説明図

第 9 図